Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 91 (2016) 412 – 421

Procedia Computer Science

Information Technology and Quantitative Management (ITQM 2016)

Managing Cloud Computing Environment: Gaining Customer Trust with Security and Ethical Management.

Issam Kouatli[a,*]

[a]**Issam Kouatli, Lebanese American University, School of Business – ITOM Department, Beirut, P.O. Box: 13-5053, Lebanon**

Abstract

This paper aims to find out the management best practices of new hype of technology like Cloud computing. The management of such environment is highly dependent on the trust relationship between the cloud service providers and their customers (and/or other businesses). This trust is not only dependent on the latest technological tools, but rather also dependent on the management strategy in such highly critical environment. To achieve this objective, a survey was conducted related to the acceptability of the cloud services which has resulted in three main sections. These were: security, data protection and ethics in cloud computing environment. The sample size was 441 where it was resulted in highly significant relationship between ethics and security as well as ethics and data protection which are the main two motivations for any business to join the cloud. Based on this study, a guideline of managing cloud computing to maintain these three issues was described. Ten steps were proposed to protect cloud services from possible unethical behaviors as well as to protect systems from possible security breach.

Peer-review under responsibility of the Organizing Committee of ITQM 2016

Keywords: Cloud Management; IT Ethics; peopleware problems; Cloud ethics; BYOD mobility policy; data protection management; security management

1. Introduction

Managing and monitoring resources of complex systems like Cloud computing is not an easy task. Improper management will lead to degradation in performance and consequently affects the trust relationship between cloud service providers with their customer. Trust would be the main pillar towards gaining successful business of cloud service providers and which is one of the main areas of interest in this paper. This trust can only be established via implementations of appropriate business processes including security management, data storage management and ethical management and monitoring of IT professionals working in such environment.

* Corresponding author. Tel.: +961-1-786-456 ; fax: +961-1-867-098 .
E-mail address: Issam.kouatli@lau.edu.lb.

Peer-review under responsibility of the Organizing Committee of ITQM 2016
doi:10.1016/j.procs.2016.07.110

Complex policies and procedures of human resources – including ethical behavior management and monitoring- would be needed to maintain technical resources in a highly demanded secure environment.

Irrespective of the offered cloud services (IaaS, SaaS, or PaaS), specific suitable procedures would be required to balance the ethical behaviors, preventing any possible insider attack as well as technical management to prevent any loss of data or any kind of hacker's attack. This paper serves two objectives: the first describes the result of a survey where high association between ethics, security and data protection was identified. The second objective proposes an appropriate business procedures and policies that can be beneficial towards maintaining the three main trust variables of data protection, security and ethical behavior.

Needless to mention about the benefits of cloud services to corporates which has been published by many researchers, for example, Kornevs et.al. [1], evaluated cloud computing from financial perspective. However, although cloud computing has an excellent financial impact to any corporate, trust would be the main motivations towards adopting the cloud for any SMBs and/or large multinational enterprises (MNE). Gaining trust in any kind of information systems including cloud computing from the customer perspective would be very important. For example, Kim et.al [2] explored the consumer perception of quality provided by new technology with a little attention to information system structure. Their study concentrated around three factors, the perceived quality, perceived usefulness and perceived risk. Resource management in terms of skills needed and disciplined behavior is an important role towards keeping cloud computing environment safe and secure. As Privacy and security were the main inhibitors of cloud adoption, Whitley et al [3] reviewed the business and legal risks associated with cloud computing. Resource management from the perspective of load balancing and identifying the peak and low demand of IT resources has recently been tackled by researchers like Weingärtner et al [4], where they have surveyed the cloud resource management to identify the most suitable amount of resource for each workload. Their paper presents a comparison of models and tools in such environment. Also, Wang et al [5] surveyed different enterprise cloud service architecture for cloud service platform and applications with emerging challenges in enterprise context. Hu et al [6] investigated the cultural effect of accepting technology in general and how it impact on the individual behavior accordingly. Based on cultural background of different individuals, I.T. ethical behavior within such environment of cloud computing is becoming a necessity before adopting cloud computing services. Cloud service providers will have to prove to their clients that data and applications are secured with ultimate protection mechanism. The heart of this protection stems from individuals' ethical behavior and as such cloud service providers has to ensure that all their staff and IT professional behaving ethically according to a preset IT code of ethics at all times. Setting the cloud services securely and developing the trust relationship between businesses and their cloud service provider is only half the story. Trust between employees and businesses in the new era of "Global Mobile Computing" would also be necessary.

Mobile devices like iPhone and tablets would add complexity to secure and protect the business from any possible malicious behavior. The challenge of securing mobile devices is in the fact that these devices are owned personally by employees which mainly used for personal usage. However, the very same device is also used by the employee/IT staff to conduct business task and hence some sensitive business information may be stored in these devices. In this case, a possible leak of business information might occur. BYOD (Bring Your Own Device) is a recent terminology used to define the usage of personal device in business environment. BYOD usage would add complexity of code of ethics development and its obvious consequences to security issues and/or the generation of any related policy development. In spite of all kinds of released policies and regulations to IT ethical behavior, the ethical dilemma may evolve in line with the advancement in information technology. Ethics has always been part of efficient productivity or performance. For example Cowton [7] examined the ethical decision making for security Service Company in England where ethical criteria with its implementations was described. Also, as typical IT professional's behavior influenced by cultural background, Cowton and Cummins [8], for example, described the identified ethical challenges as a baseline for developing

future business ethics. Such dilemma is more enhanced when it comes to IT ethics in specific. The impact of unethical IT behavior to businesses in general and to businesses joining the cloud computing services in specific was reviewed by Kouatli [9]. Historical review of IT vulnerabilities as technologies emerged was also studied by Kouatli [10, 11]. There are many papers that review the type of damage as a result of illegal/unethical behaviors. For example, Svensson and Wood [12] proposed a business ethics model based on 3 components, expectations, perceptions and evaluations. Siu et al. [13] provide a comparative study of ethics between managers and non-manager. Needless to mention that the impact of unethical behavior, if not controlled and monitored, might lead in some situations to tremendous amount of possible malicious behavior.

This paper discusses three main issues. The first section deals with the peopleware problems and suggestions to avoid/reduce the unethical "peopleware" issues. The second section discusses the result of a Cloud Computing survey where all participants were students already educated about Cloud Computing. The survey, analyze three main issues: Security, Protection and Ethics in Cloud computing environment. As network security management is essential part of protecting any business, CISCO [14] recommended managerial action of best practice protection of network in a technical environment. In an analogy of this document, the third section establishes the best practices guideline to secure and protect new technological environments like cloud computing services.

2. Peopleware Problem and The Need for Cloud code of Ethics

As IT ethics is in a process of continuous development whenever a new technology emerges, policy and IT code of ethics also needs to be updated and examined before adoption of such technology. Many researchers were interested on the issue of ethics in IT environment. For example, Kallman et al [15] explain that the primary steps to cultivate an ethical computing environment are constructing rules of conduct and code of ethics. Maner [16] also highlights the fact that the use of computers/IT transformed some business ethical issues into a radically altered form of ethics. Hence, businesses must have a code of ethics not only for their general business behavior but also specific IT ethics rules and policies. The creation of IT ethical commandments witnessed several attempts, but due to the absence of a centralized and authoritative body governing the IT world, it proliferated independently. So we now have different lists of "commandments", each one is self-proclaimed as exhaustive. Many IT groups in several places came together to outline their understanding of IT ethics. One was created by the Computer Ethics Institute and named "the Ten commandments of Computer Ethics" as an analogy of the Ten Commandments of the Bible. Several other lists were also created by different institutes like ACM [17] and BCS [18], but only the most popular code of ethics is usually taken proper analysis.

The main reason for implementing code of ethics is to manage employee behavior. A code of ethics is a common organizational policy used in business organizations. The code of ethics policy usually sets the minimum standards for business owners, managers and employees to follow when completing various business functions. When employees fail to behave ethically, managers must quickly react to deal with the bad behavior otherwise, inappropriate behavior might spread throughout your business. A code of ethics would be necessary to maintain issues of confidentiality, efficiency and acting as a protective measure against possible unethical behavior.

3. Added Complexity of Cloud Computing services

Reduction of IT infrastructure and/or operational cost could be the main motivation for corporates to acquire a cloud computing services. These benefits do not come without obstacles that need to be addressed. Usually there are two different types of clouds, Public and Private. Most corporates would utilize a hybrid cloud where they host most of their insensitive applications and data in the public cloud and secure their sensitive data and

application in an in-house built private cloud (corporate Data centre). Cloud computing services would add the complexity of managing and maintain a good ethical and/or secure environment. For example, different IT professionals assigned to serve different groups of clients in a cloud computing service providers' company. In traditional IT environment for a specific business, it is usually normal that some IT professional exchange the administrative passwords whenever necessary to ease the process of administration. This might not be acceptable in some cloud service provider companies where clients might be competing businesses in the same industry. Special Cloud ethics has to be developed to maintain ethical and secure environment for the service providers' clients.

Also, the issue of accountability of day-to-day tasks done by IT professionals in service provider's environment has to be addressed. It is of utmost necessity to prove to businesses that their data and applications are secured at all times by tracking the individuals whom are responsible for maintenance, backup…etc. As part of data protection, this might include data replication. At any moment in time, businesses have the right to know the location of all replicas of their data. This might not be an easy task as the system will be automated to replicate the data to different locations. In some cases the IT professional would not be able to exactly locate all replica that may exist somewhere around the globe. Additional issue related to data replication is that one of the replicated data might be located in a country where IT ethics is not respected and legislation is not clear (if exists). This would be an added vulnerability of client's data to be lost or stolen in a country with no legislation (or at least no clear law) against such act.

The added complexity of cloud computing forces a revisit on the IT code of ethics and possible definition of a new "Cloud" code of ethics would be necessary. Cloud ethics in this case can be very beneficial to cloud service providers to adopt in order to maintain the trust relationship between them and their clients (businesses).

4. Cloud computing acceptability survey

4.1. Methodology

An acceptability survey of cloud computing was conducted where all participants were university students with adequate education about cloud computing. In general, five main sections were investigated. These are financial viability (Motivation), Availability, Security, Protection and Ethics. The study aims to focus on the three main issues which are security, protection and ethics and its relation to the possible acceptability for data storage (and management) as well as Cloud application usage. The total number of questions was 47 questions split into the following sections:

1-Motivation Section (financial viability): Eight different questions related to general Acceptability of Cloud computing (mainly in terms of business benefits, ROI reduction…etc.)

2-Protectability Section: Sixteen different questions related to protection issues like Data recovery in case of loss, data protection during transmission as well as data storage protection.

3- Security Section: Nine questions related to security issues like storage of data on shared medium, encryption and IT professional ability to secure the environment.

4- Availability Section: Four questions related to Availability issue of cloud computing. For example data availability, even if the cloud service provider went broke, the expectation of robustness level of the connected devices as well as the reliability of fault-tolerance mechanism

5-Ethical Section: Eight Questions related to ethical issues within the cloud environment like following the code of ethics with clear policy and actions in case of violations.

The last two questions are dependent variable answering "yes" or No" to the overall acceptability to use the cloud for Applications (question 46) and Data storage (Question47) respectively.

The target population were MIS students from a single university located in the middle-east. These participants are educated in MIS in general and in Cloud computing in specific as part of their course study in

the business school. The sample was taken from the student classrooms. Although the sample is only based (biased) from one geographical location and in specific from one university, however, it does show a possible trend of how potential customers think/ trust cloud. Hence, statistics can only show an indicator about the importance of ethics in terms of protection and security of cloud computing.

4.2. Observation and data analysis

The main purpose of this survey is to observe and identify the most influencing factors related to Data Protection, Security and ethics in a cloud computing environment. Then the second objective is to identify which of these three major criteria would be an influencing factor towards acceptability of cloud services in terms of averaged output of protection, security and ethics sections. Looking at figure 1 describing the Data Protection section, it can be noticed that about 80% of participants are reluctant to use Cloud services to store their personal data (Q9) where it is more acceptable to them to store their customer and/or financial data (Q10 and Q11). This would be related to personal privacy issue as most people would like to keep their personal details confidential (Q13) and it seems they do not have full trust that cloud service providers would be able to maintain their privacy and protect their personal data. Unexpectedly, it is fairly acceptable for them that their customer data and financial data to be managed by cloud service providers. Moreover, out of the sixteen questions regarding protection section, 60% of participants prefer to know the exact location of their data storage (Q12) in the cloud. This can be explained due to the worries about integrity of their data as well as ability to investigate incidents with an existing support from authorities which is indicated by (Q15 and Q24).

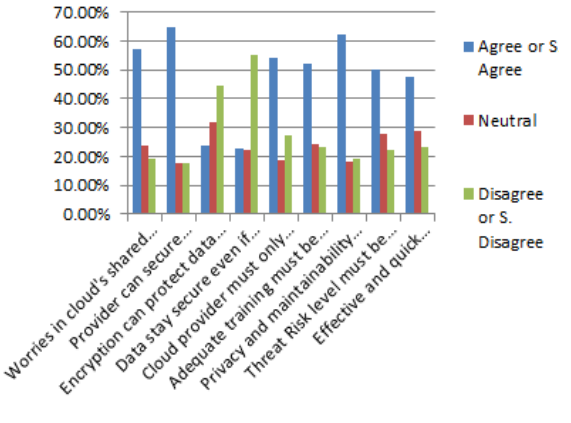

Fig. 1- Histogram for the data protection section (Q9-Q24)

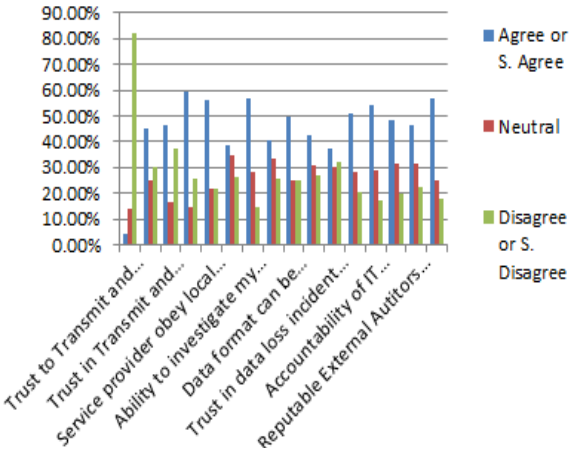

Fig. 2- Histogram for the security section (Q25-Q33)

Looking at figure 2, out of the 9 questions related to security, the most desired item would be to secure their data on the shared medium (Q25 and Q26). This type of security is intersected with data protection where participants are still worried about their data being compromised and the typical solution of encryption to protect their data. This coincides with the next highest response by participants which is the IT professional ability and ethics to maintain their data (Q29, Q30 and Q31). Moreover, it seems that participants do not trust that their data will stay being secured (about 55%) if the cloud service provider company got acquired by another company (Q28). Ethical Issues and concerns are represented in "IT Ethical Section" which is summarized in figure 3 which shows that participants are worried when it comes to the same professional servicing their data as well as their competitor's data (Q39). This would be applicable when businesses worried about leakage of sensitive data and information to their competitors. The other major concerns are that

participants prefer that the IT professionals are well trained/certified in ethical behaviour and they follow the IT code of ethics (Q38). Also, Policy and disciplinary actions in case of any violations should be clearly highlighted by service providers in case of any violation (Q45).

Figure 4 shows the summary of all three sections (Protectivity, Security and Ethics) by averaging each section and the overall acceptability for data usage and application usage respectively (Q46 and Q47). It indicates that 70% of the populations do not mind to use Cloud for application usage but they are reluctant to use cloud for Data storage and management (about 49%). Ethical concerns represent the most influential factor.

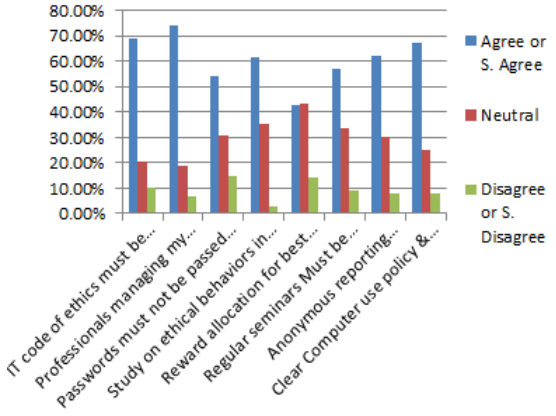

Fig. 3- Histogram for the IT Ethics Section (Q38-Q45)

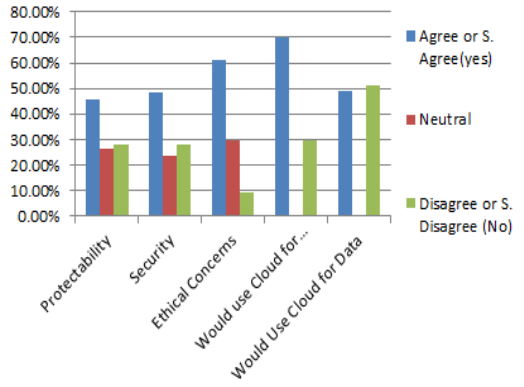

Fig. 4- Histogram for the averaged values of all sections

The calculated Margin of error for each of the three main variables are shown in Table1 presenting the means,, and standard deviations and Margin of Error for each one of the variable using confidence level of 95%. All the variables have means slightly higher than the centre of their range (1.0 to 7.0) which means that participants favour high level of data protection and security when questioned. In specific the Ethics mean was 5.37 indicating a high emphasis of ethics in relation to security and data protection.

Moreover, regression analysis between ethics and security (Figure 5) shows high association between them with a modest R=0.565 (R^2=0.319) significant at 1%level. Also, regression analysis between ethics and data protection (figure 6) shows a modest relationship of R value of 0.548 (R^2= 0.299) with <1% significance.

Table 1.Summary of mean and Margin of error for each one of the variables at 95% confidence

	Conf. Level	Mean	Std. Dev.	Z	Margin of Error
Averaged Security	95%	4.57	1.14	1.96	+/- 0.106
Averaged Data Protection	95%	4.51	1.02	1.96	+/- 0.095
Average Ethics	95%	5.37	1.101	1.96	+/- 0.103

5. Avoiding peopleware problem

Most of the unethical/illegal IT attack techniques are usually insiders based attacks committed by unsatisfied employee(s) having unethical behaviour triggered by a situation in their working environment. This is a usual case of peopleware problem which was first introduced by Neumann [19]. Sociological and political problems have to be addressed by organization to avoid such destructive possibility. To rectify and minimize this unethical behaviour, it would not be enough to counterattack the malicious techniques by using anti-virus technology/techniques. Proper management would be necessary to rectify any possible problem in unethical IT

behaviour. Therefore, the issue is not only the malware technology, but it is rather “peopleware problem” (Shaw et al [20]). Since the people are behind the creation and attack of the same systems, it would be necessary to conduct psychological analysis of the information systems criminals, in order to safeguard those systems.

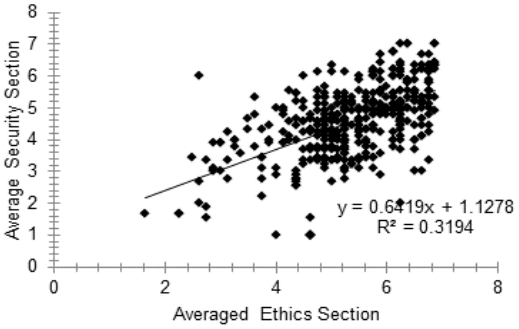

Fig.5- Regression analysis for security and ethics

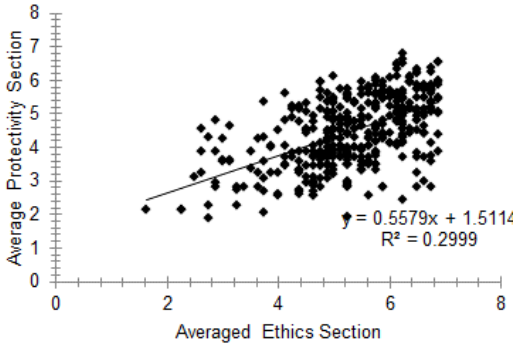

Fig. 6- Regression analysis for data protection and ethics

In face of this huge problem created by IT, the IT professional community rushed to create norms to give orders and moral structure to the chaotic situation. One primary and essential tool was to create a robust body of guidelines, norms, measures and rules regulating the outside professional community. One of the earliest ones was The Ten Commandments of Computer Ethics as stated by Ramon [21]. A more comprehensive cloud tailored Ten Commandments were proposed by Kouatli [22]. One of the major parts of the commandments was to highlighted ethical behavior in an IT environment to all staff and IT professionals. Although IT professionals usually have ethical education in their perspective schools, a gap does exist between their theoretical knowledge and practical behavior. Employees in general and IT professionals in particular must be surveyed to find and analyze such a gap. Then, an awareness seminar/campaign must be provided to the staff to maintain appropriate IT ethical behavior and security policy implementation to protect the businesses. Surveying all employees/IT Staff via questionnaires would provide good indicators about the level of ethical behavior conducted in the business environment. A similar study was conducted by Kouatli & Balozian [23], where the objective was to compare the individual’s theoretical knowledge about IT ethics as compared with the practical ethical behavior in business environments. This study discovered that 33.6% of the employees wouldn’t inform their supervisors about possible faults that might damage the whole system. This shows that participants usually worried that their reputation (not to be seen making mistakes) prioritized over the success of their company tasks. Moreover, statistics revealed that members in a team were careless when it came to change their password when noticed by coworker(s) (“shoulder surfing”), A surprising more than two third (65%) would not change the password in such cases. This shows that the attitude of staff favors friendship over security. Although this indicates good trust and team bonding in business working environment among employees, however, employees might be violating the security policy of the company. Managers should plan for dissemination of cloud code of ethics on employees enforcing them to obey the policy to the letter. The following steps can be proposed:

Step 1: Collect Information and compare the existing policy with the company mission and working environment. Also, Survey all employees to gather all concerns of about any ethical issues.

Step 2: Clarify any unclear statements in the mission, objectives or Policy to include ethical review and/or internal ethical audit among employees. Comprehensive and clear policy must be clearly advertised on the organization's intranet where all employees should sign on the ethics policy.

Step 3: Provide ethical training in form of cases and scenarios to learn from. Moreover, effects of wrongdoing to the business in general and to individual specifically must be explained. The fine line between good team bonding and friendship versus strict implementation of the policy should be explained. Regular mandatory workshops would also be necessary to discuss emerging ethical issues

Step 4: Encourage team bonding for enhanced team performance but at the same time encourage employees to come forward and report wrongdoings of any other member in his/her team.

Step 5: In order to help employees to come forward and report any wrongdoing, an anonymous reporting system must be established to help employees communicate breaches of the ethics plan. This would be necessary to avoid any kind of conflict among employees by reporting on each other. Also, employees will always behave ethically as they don't know who might be reporting on them.

6. Managerial actions to protect businesses

On top of technological solutions, a good management strategy would need to be implemented effectively. Cisco white paper [14] for example, suggests security best practices to protect their organizations. To protect cloudy businesses, as similar approach must be followed as identified in the following ten steps formatted as 3 main criteria and 10 sub-criteria summarizing the actions required to achieve a good practice to protect cloudy businesses. These criteria are generic to most technical environment in general and to cloud computing environment in specific.

6.1. The policy criteria

Step1-Clarity Sub-Criteria: It is necessary to create a Computer-Use policy that states what employees allowed to do or not do. This policy should be well advertised in the Cloud service provider professionals clearly highlighting the consequences of violating the policy with disciplinary action/procedure in case of violation.

Step2- Acceptability Sub-Criteria: The above policy may also include a statement to clarify the partner "Acceptable" use of the IT systems in your business. It should clearly state the consequences to them in case a security attack has happened.

Step3- Plan-ability Sub-Criteria: The above policy must also include an acceptable use statement for administrators/IT staff. It should explain the procedure of policy enforcement, privilege review and user account administration. This should be reflected in the training plans and evaluations of the IT staff.

6.2. The Risk analysis criteria

Step4- Threat Detectability Sub-Criteria: Identify sections of your network/systems with the possible threat rating for each section. Then you can identify the required level of security in each section. This would help in balancing between tight security with slow performance and low security sections with high performance. Risk level must be evaluated and assigned to each of the following: main network devices, network monitoring devices, distribution network devices, access network devices, network security devices (if any), e-mail systems, network file servers, network print servers, network application servers (DNS and DHCP), data application servers (Databases), desktop computers, and other devices (standalone print servers and network fax machines).

Step5- Monitoring Access-ability Sub-Criteria: Identify the types of users of that system with different access level: Administrators, privileges and general user. These must be tracked at any time when authorized systems used.

6.3. Team-Performance Criteria

Step6- Policy Reviewability Sub-Criteria: Security team must be led by a team leader where the team is composed of employees representing different operational departments. They should be aware of the security policy and the technical aspects of security design and implementation and hence, proper training would be required for the team members. The security team has three main responsibilities: The policy development to establish and review policies, practice to conduct the risk analysis with possible change requests and response to possible threats and to fix any violations. The individual roles and responsibilities of the security team members in your security policy must be defined with clear description.

Step7- Changeability Sub-Criteria: Approving Security Change: Your security policy should identify specific security documentation in non-technical terms. The security team should match this non-technical document into technical security configuration document. Then, you can apply these to any future configuration changes.

Besides these approved guidelines, select a member from the security team to sit on the change management approval committee to monitor any possible changes.

Step8- Response-Ability Sub-Criteria: Security Violations: Monitoring the security of your network. It is recommended that monitoring low-risk equipment weekly, medium-risk equipment daily and high-risk equipment hourly is essential. Your security policy should address how to notify the security team for security violations. This can be automated via the network monitoring software that can be capable of sending SMS or similar notification to security member in case of violation. Quick decisions when a violation is detected are crucial to system recovery. The first action in this case would be the notification of the security team at any time within the 24 hours. This should be reflected in your security policy. Moreover, the level of authority given to security members should be clearly defined.

Step9- Maintainability Sub-Criteria: Collect and maintain information during a security attack. Details about the compromised system must be logged to form the basis of possible prosecution of external violations. Your legal department should review the procedures for gathering evidence in case of legal action to be taken.

Step 10- Restore-Ability Sub-Criteria: As each system has its own procedure of backing up, security policy should define how you conduct, secure, and make available normal backups.

7. Conclusion

In this paper, Trust relationship in cloud computing environment was investigated. Data Protection, security and ethics were the most significant variable in the conducted survey. Trust relationship would be the main factors before cloud computing acceptability by SMBs in general and for MNEs in specific.

Observational and data analysis were discussed where the results shows strong associations between the data protection, security and ethics in cloud computing environment. As a result of the observational analysis, this paper also proposes an IT managerial guideline of cloud service technical environment. This guideline proposed in a form of steps towards managing IT professionals (Peopleware problems) as well as management of IT staff in a technical environment like cloud computing to avoid any possible breach of security and/or data loss that are mainly driven by unethical behaviours. The proposed guideline is becoming a necessity due to the new cloud computing environment and I.T. globalization. The guideline presented in a form of three main criteria which has been defined in ten different sub-criteria (steps) to achieve security and data protection.

References

[1] Kornevs M, Minkevica V, Holm M. Cloud Computing Evaluation Based on Financial Metrics. Information Technology and Management Science 2013; 15(1): 87–92.
[2] Kim J, Yuan X, Kim S, Lee Y. How Perceived Quality Works in New Technology Adoption Process: A Cross-National Comparison among China, Korea and Japan. Journal of Global Information Management 2014; 22(2)
[3] Whitley E, Willcocks L, Venters W. Privacy & security in the Cloud. Journal of International Technology and Information Management. 2013; 22(3)
[4] Weingärtner R, Bräscher G, Westphall C. Cloud resource management: A survey on forecasting and profiling models. Journal of Network and Computer Applications 2015; 47: 99-116.
[5] Wang H, He W, Wang FK. Enterprise cloud service architectures. Information Technology and Management 2012; 13(4): 445-454.
[6] Hu P, Eccles D, Al-Gahtani S, Hu H. Arabian Workers' Acceptance of Computer Technology: A Model Comparison Perspective. Journal of Global Information Management 2014; 22(2)
[7] Cowton C. Playing by the rules: ethical criteria at an ethical investment fund. Business Ethics: A European Review 1999; 8(1): 60-69
[8] Cowton C, Cummins, J. Teaching Business Ethics in UK Higher Education: Progress and Prospects. Teaching Business Ethics 2003; 7(1): 37-54.
[9] Kouatli I. Impact of unethical IT behaviours to cloudy businesses. International Journal of Trade and Global Markets 2014; 7(3)
[10] Kouatli I. A Comparative study of the evolution of vulnerabilities in IT systems and its relation to the new concept of Cloud computing. Journal of Management History 2014; 20(4): 409-433
[11] Kouatli I. Global business vulnerabilities in cloud computing Services. International Journal of Trade and Global Markets, 2016; 9(1)
[12] Svensson G, Wood G. A Model of Business Ethics. Journal of Business Ethics 2008; 77(3): 303–322
[13] Siu N, Lam K. A Comparative Study of Ethical Perceptions of Managers and Non-Managers. Journal of Business Ethics 2009; 88(1): 167–183
[14] CISCO. Network Security Policy: Best Practices. White Paper- Document ID: 13601
[15] Kallman EA, Grillo J. Ethical decision making and information technology: An introduction with cases. McGraw-Hill 1998; 29-109
[16] Maner W. Unique Ethical Problems in Information Technology. Science and Engineering Ethics 1996; 2(2): 137-154.
[17] ACM: The Association for Computing Machinery (ACM), http://www.acm.org/about/code-of-ethics/
[18] BCS: The British computer society code of conduct, http://www.ccsr.cse.dmu.ac.uk/resources/professionalism/codes/Bcs.html
[19] Neumann P G. Peopleware in Systems. Cleveland, OH: Assoc. for Systems management, 1977: 15-18.
[20] Shaw E, Ruby K.G, Post J.M... The Insider Threat to Information Systems. Security awareness Bulletin 1998; 2(98): 1-10.
[21] Ramon C. B. In pursuit of a 'Ten Commandments' for computer ethics. Computer Ethics Institute. 1992. Retrieved from: http://computerethicsinstitute.org/publications/tencommandments.html
[22] Kouatli I. The Ten Commandments of Cloud Computing Security Management. International Conference on Cloud Security Management (ICCSM) 2014; 73-81
[23] Kouatli I and Balozian P. Theoretical Versus Practical Perception of IT ethics in Lebanon. Society of Interdisciplinary Business Research (SIBR) Conference 2011